CONTINUATION IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Andrew DeCoster, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since 2018 and am currently assigned to the Detroit Division. My duties include the investigation of alleged violations of federal criminal laws, including matters involving violations of 18 U.S.C. §§ 2252A(a)(2), which makes it a crime to receive or distribute child pornography in, or using a facility of, interstate or foreign commerce; and 2252A(a)(5)(B), which makes it a crime to possess or knowingly access with intent to view child pornography. These items are more particularly described in Attachment B.

2. Pursuant to the provisions of 18 U.S.C. § 2256(8), "child pornography" means a visual depiction, the production of which involves the use of a minor engaging in sexually explicit conduct, including but not limited to various simulated or actual sex acts, or the lascivious exhibition of the genitals or the pubic area.

3. This continuation is submitted in support of an application, under Rule 41 of the Federal Rules of Criminal Procedure, for a search warrant for the locations specifically described in Attachment A, including Yahoo email account **edchora@yahoo.com ("Target Account")**. There is also probable cause to search

the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

4. The statements contained in this continuation are based in part on information provided by U.S. federal law enforcement agents, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement officers, information gathered from investigative sources of information, and my experience, training, and background as a Special Agent.

5. This continuation is submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of federal law are located at the **Target Account.**

FACTUAL BACKGROUND OF INVESTIGATION

6. On March 23, 2022, Victim 1[1] submitted an online tip to the FBI National Threat Operations Center (NTOC) indicating she was being extorted for explicit photos by someone who referred to himself in online interactions as "Chris Medina."

7. On March 25, 2022, I interviewed Victim 1 telephonically. When Victim 1 was approximately 16 or 17 years old, approximately in 2017, she sent sexually

[1] Victim 1's full name is known to me, but I have omitted that information to protect her identity.

explicit images to the person she knew online as "Chris Medina" via Instagram and Snapchat.[2] Originally, Victim 1 communicated with Medina through the Instagram account here_we_stand_9. At least one of the images included nudity when she was a minor. Medina threatened to kill himself if Victim 1 did not send sexually explicit photographs of herself. After approximately six months from the first interaction with Medina, Victim 1 blocked accounts attributed to Medina.

8. In a later interview, Victim 1 said she took at least ten sexually explicit photos of herself when she was under the age of 18 and sent them to Medina. Some of the photos included her bare breasts. Other photos were nude photos of her genital area. Medina directed Victim 1 to pose in some of the pictures. Victim 1 remembered posing in the bathroom on a sink with one of her legs up, as well as taking photos "from the back" and "laying down."

9. Since 2017, other accounts, suspected to be Medina, attempted to extort Victim 1 for more sexually explicit photographs. Those accounts threatened to send Victim 1's sexually explicit images to her friends, co-workers, and family members if she did not send photographs and/or videos of Victim 1 and her current boyfriend having sex.

[2] Snapchat and Instagram are social media platforms that allow users to share moments with photos, videos, and chats/messages. More detailed background information regarding Instagram and Snapchat is provided in the separate background sections below.

10. On March 29, 2022, Victim 1 identified Snapchat accounts j_st22738, jkl_ll2022, and jkolivia22 as being attributable to the person she knew as Medina. Victim 1 identified Instagram accounts here_we_stand_9, olivia9994916, and slayeer8 as being attributable to Medina. Victim 1 suspected these accounts were attributable to Medina due to common language and topics of conversation, including references to previous explicit photographs and threats to expose the photographs. Additionally, on one account, the user indicated he would keep making "ghost accounts."

11. On April 5, 2022, I interviewed Victim 1 at the FBI Lansing Resident Agency. Victim 1 reiterated she was under the age of 18 when she sent sexually explicit photos (including of her genital area) to Medina. Victim 1's father provided a flash drive that contained messages between Victim 1 and a user suspected to be Medina.

12. A review of the flash drive included screenshots of a conversation between Victim 1 and a Snapchat profile attributed to be Medina—account j_st22738. Medina said, "And i have a lot … Of pics even ones that u sent that show your face." Medina said, "[First name of Victim 1] u sent me a shit load when we were together." Victim 1 replied, "I was also a minor," to which Medina replied, "U know i have them i even showed ur ex friend or friend who was in the military [sic]."

13. Victim 1 was last contacted by Instagram account slayeer8, attributed to Medina, on or about May 23, 2022. In the conversations, Medina said, "do you

think [relative of Victim 1] will like your nudes … or lee .. Madison." After Victim 1 responded, Medina said, "your step dad might like them … [relative of Victim 1] might get a kick of them … lets find out."

14. Victim 1 also identified Victim 2[3] as another victim of Medina. According to Victim 1, several years ago, Victim 2 texted Victim 1 to "back off" Medina because they were in a relationship together. At an unknown date later, Victim 2 apologized to Victim 1 and said she was also manipulated by Medina.

15. On April 12, 2022, I interviewed Victim 2 at the FBI Lansing Resident Agency. In approximately 2017, Victim 2 was 17 years old and received a message from a person who identified himself online as "Chris Peterson" via Instagram account here_we_stand_9—the same Instagram account that Victim 1 used to communicate with "Chris Medina." Victim 2 told Peterson she was 17 years old. Victim 2 also communicated with Peterson on other Instagram accounts and on Snapchat account **ek1572** for approximately four and a half years when they were in an online relationship.

16. Victim 2 indicated she sent sexually explicit photographs of herself to Peterson over Snapchat. Peterson instructed Victim 2 to "do things," which included masturbation. Victim 2's pictures were "very nude," and included pictures of her breasts and "lower parts," by which I believe she means her pubic area. Some of these

[3] Victim 2's full name is known to me, but I have omitted that information to protect the identity of the victim.

photographs were taken when Victim 2 was under 18 years old. Peterson threatened to break up with Victim 2 if she did not send sexually explicit photos to him or find two other people to have sex with on camera. Victim 2 later broke up with Peterson and blocked his accounts.

17. Peterson also sent Victim 2's sexually explicit photographs to Victim 2's mother via Snapchat.

18. On April 12, 2022, I interviewed Victim 2's mother at the FBI Lansing Resident Agency. Victim 2's mother provided copies of conversations between her and Peterson.

19. Victim 2's mother identified Instagram accounts here_we_stand_9, jamesrr729, killaman4589, killabea3, killalocr, systemdown18880, and jame.sr3675 as attributable to Peterson. Victim 2's mother identified Snapchat account ek1572 as attributable to Peterson. Victim 2's mother identified Kik[4] account EasyE81 as attributable to Peterson. Victim 2's mother attributed all the identified accounts to the person she knew as Peterson due to the context of the conversations, specifically regarding the ability to post pictures of Victim 2, and the continuation of discussions across the various accounts.

[4] Kik is a smartphone messenger application that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos and more – all within the app. Kik is available for download through the iOS App Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Users may also be using Kik on their Windows, Symbian-based or BlackBerry OS. Kik is free to download and uses an existing Wi-Fi connection or data plan to send and receive messages.

IDENTIFYING "CHRIS MEDINA"/ "CHRIS PETERSON" AS EDUARDO CHORA

20. For the reasons outlined in this section below, law enforcement has identified Eduardo or Ed Chora as the person the victims knew as "Chris Medina" and "Chris Peterson."

21. Based on the information provided above from Victim 1, Victim 2, and Victim 2's mother, on or about April 15, 2022, investigators served an administrative subpoena on Snapchat for subscriber records of accounts j_st22738, jkl_ll2022, jkolivia22, and ek1572.

22. On or about May 4, 2022, Snapchat responded with subscriber information and Internet Protocol (IP) logs for accounts j_st22738, jkl_ll2022, jkolivia22, and ek1572. Snapchat's response included email addresses and captured IP logs for all requested accounts. Email addresses gijoey851@gmail.com and edchora63@gmail.com were attributed to account ek1572. Email address edchora63@gmail.com was attributed to account j_st22738. Email address gijoey@gmaip.com, entered with the misspelling of "gmail," was attributed to account jkl_ll2022. Email address juanrambo035@gmail.com was attributed to account jkolivia22.

23. I am aware that Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller

pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.[5]

24. According to the IP logs provided by Snapchat, accounts j_st22738, jkl_ll2022, jkolivia22, and ek1572 all logged into IP address 52.144.117.168 on March 24, 2022. A search of the internet revealed IP address 52.144.117.168 was registered to MetroNet Inc.

25. Additionally, on or about April 15, 2022, investigators served an administrative subpoena on Meta Platforms Inc., the owner and operator of Instagram, for subscriber records of accounts here_we_stand_9, Olivia9994916, Slayeer8, jamesrr729, killaman4589, killabea3, killalocr, systemdown18880, and jame.sr3675.

26. On or about May 20, 2022, Meta Platforms Inc. (Instagram) responded with subscriber information and IP logs for accounts here_we_stand_9, Olivia9994916, slayeer8, jamesrr729, killaman4589, killabea3, killalocr, systemdown18880, and jame.sr3675. Meta Platforms Inc.'s response included the email address juanrambo035@gmail.com for several of the accounts, and captured IP logs for the identified accounts. As discussed above, email address

[5] https://www.cloudflare.com/learning/network-layer/internet-protocol/

juanrambo035@gmail.com was also identified in Snapchat's May 4, 2022 subpoena response.

27. According to the IP logs provided by Meta Platforms Inc. for the identified Instagram accounts, the IP address used for the creation of accounts slayeer8 and olivia9994916 was the same IP address used as logins for Instagram account jamesrr729. Additionally, the IP address used for the creation of account olivia9994916 was the same IP address used for the Snapchat account creations of jkolivia22 and jkl_ll2022.

28. A review of Snapchat and Meta Platforms subpoena returns also revealed that IP address 209.249.25.60 was captured as account activity associated with slayeer8 (Instagram), jamesrr729 (Instagram), and ek1572 (Snapchat). On or about June 8, 2022, the FBI determined that IP address 209.249.25.60 was attributable to Edward W. Sparrow Hospital Association, 1215 E Michigan Ave, Lansing, MI 48912, telephone number 517-364-1000.

29. One of the IP addresses associated with account activity j_st22738 (Snapchat) was 2607:fb90:88e4:d41e:0:8:b049:7401. On or about June 9, 2022, investigators served an administrative subpoena to T-Mobile for subscriber information of that IP address.

30. On or about June 14, 2022, T-Mobile responded with a return, stating the subscriber details for the account associated with IP address 2607:fb90:88e4:d41e:0:8:b049:7401 on March 24, 2022, at 01:50:53 UTC was:

a. Subscriber Name: Eduardo Chora

b. Subscriber Address: 3016 Pleasant Grove Rd., Lansing, MI 48910-2306

c. Phone Model: SAM A20 32G BLK TMUS KIT RSU

d. Phone Model: SAM J700T WHITE TMUS KIT RSU

31. On or about June 9, 2022, investigators served an administrative subpoena on Kik c/o MediaLab.ai Inc. for subscriber information and IP activity for Kik account EasyE81—an account identified by Victim 2's mother as being associated with "Chris Peterson."

32. On or about June 13, 2022, Kik c/o MediaLab.ai Inc. responded with subscriber information and IP logs for Kik account EasyE81. Email address gijoey851@gmail.com was identified. Under Registration Client Info, a Samsung SM-A205U was identified. The IP logs produced by Kik c/o MediaLab.ai Inc. included specific port numbers from previously identified IP addresses, including IP address 52.144.117.168, which was associated with MetroNet Inc.

33. I am aware that in computer networking, port numbers are part of the addressing information used to identify the senders and receivers of messages. They are associated with TCP/IP network connections and might be described as an add-on to the IP address.[6]

[6]https://www.techtarget.com/searchnetworking/definition/port-number#:~:text=A%20port%20number%20is%20a,that%20have%20an%20assigned%20number.

34. On or about June 16, 2022, the State of Michigan Department of Labor and Economic Opportunity provided wage records for Eduardo Chora. The wages were reported to the State of Michigan each quarter. With the quarter that ended on December 31, 2021, one of the employers listed for Chora was Sparrow Hospital, the site of several of the IP address log-ons by the solicitor described above.

35. On or about June 16, 2022, investigators served an administrative subpoena on Sparrow Health System's payroll and disbursements department for documentation of dates and times worked by Chora.

36. On or about June 17, 2022, Sparrow Health System responded with a return of dates and times worked by Chora between approximately October 1, 2021, and June 16, 2022.

37. The dates and times worked by Chora were compared to social media IP logs associated with Sparrow Hospital's open network IP address 209.249.25.60. The following accounts had IP log connections to IP address 209.249.25.60: slayeer8 (Instagram), jamesrr729 (Instagram), ek1572 (Snapchat), and EasyE81 (Kik). The IP address was recorded as account activity in these accounts on 66 unique days between October 27, 2021, and May 19, 2022. Sparrow Health's records confirmed that Chora worked for Sparrow Hospital on all 66 days.

38. On or about June 16, 2022, investigators served an administrative subpoena on MetroNet Inc. for subscriber information for IP address 52.144.117.168

Port 43416 on May 24, 2022 at 02:04:37 UTC, which was associated with Kik account EasyE81.

39. On or about June 23, 2022, MetroNet Inc. responded with a return, stating the subscriber details for the account associated with IP address 52.144.117.168 Port 43416 on May 24, 2022 at 02:04:37 UTC were:

a. Subscriber Name: Eduardo Chora

b. Physical Address: 1842 Delevan Avenue, Lansing, MI 48910

c. Phone Number: 517-703-7053

d. Email: edchora63@gmail.com[7]

40. I conducted an Accurint public records search of Eduardo Chora. The listed telephone number for Chora was 517-703-7053. One of the listed addresses for Chora was 1842 Delevan Avenue, Lansing, MI.

41. Records from the Michigan Secretary of State showed Eduardo Chora, date of birth November XX, 1991[8], has a driver's license registered to 1842 Delevan Avenue Lansing, MI. A 2015 Chevrolet Impala, MI license plate DZC6580, is registered to Chora at 1842 Delevan Avenue, Lansing, MI.

42. Using Chora's identifying information and a comparison of Chora's driver's license photo, I identified Facebook public profile "Eduardo Miguel Chora

[7] This was one of the same email addresses that Snapchat attributed to account ek1572 and j_st22738.

[8] His full date of birth is known to me, but I have redacted it to protect personal identifying information.

Santibanez," located at www.facebook.com/eduardo.m.chora, as Chora's. On June 7, 2022, that profile posted an image of a red Chevrolet Impala.

43. On June 30, 2022, investigators conducted surveillance at 1842 Delevan Avenue, Lansing, MI**.** A red sedan, similar to a vehicle observed in Chora's Facebook account, was pulled into a parking spot directly behind 1842 Delevan Avenue, Lansing, MI. On July 6, 2022, surveillance identified a red Chevrolet Impala, MI license plate DZC6580, registered to Chora, parked in the driveway south of 1842 Delevan Avenue, Lansing, MI.

44. On July 29, 2022, the FBI sent Yahoo! Inc., a preservation request for the **Target Account**, and they provided reference number 525992.

45. On July 19, 2022, United States Magistrate Judge Sally J. Berens granted a search warrant application for 1842 Delevan Avenue, Lansing, MI. (See In re: 1842 Delevan Avenue, Lansing, Michigan 48910, 22-mj-321.) During the search warrant execution on July 29, 2022, Chora was interviewed regarding his conduct and the email addresses, online aliases, and screen names across the various platforms. Specifically, with respect to Yahoo, he provided **edchora@yahoo.com (the Target Account)** as his email address. When later asked during the interview about "the images [he] received from [Victim 1] and [Victim 2,]" and if they could be located at Chora's email address **edchora@yahoo.com**, Chora agreed and said, "mmm hmm." Later when asked again if "**edchora@yahoo.com** would be where the majority of the photos would be kept," Chora said, "yes sir."

46. Approximately one hour and twenty minutes into the interview, Chora stated, "I'll admit to everything here, okay" and "I did it all. I fucked up." In summary, Chora indicated throughout the interview that all the identified email addresses, aliases, and screen names across the various platforms were his, including the **Target Account**.

47. On August 10, 2022, Chora sent an FBI agent an email regarding the search warrant and interview that occurred on July 29, 2022. In the email, Chora wrote, "… and I was so scared the date I meet you knew I agreed to things I didn't do…"

48. A cellular phone attributed to Chora was seized during the search warrant execution at 1842 Delevan Avenue. The FBI's cursory review of the phone showed email address edchora63@gmail.com logged into the phone. The cloud-based backup on the phone was not enabled. The FBI did not observe any images of Victim 1 and Victim 2 during this initial review of the phone data. The phone has been sent to the FBI's Computer Analysis Response Team (CART) for complete device examination.

49. With respect to this cellular phone, Chora said in his interview during the search warrant execution that he and his wife recently both got new phones when Chora began working at Walmart "a few weeks" ago and that Chora's wife threw away the old phones when they purchased the new ones. Chora told investigators that his old phone was backed up on his new phone via the Google cloud at his email

address edchora63@gmail.com. As discussed above, the FBI determined that the cloud backup was not enabled, but the phone was logged in with the email address edchora63@gmail.com. In my training and experience, given the lack of cloud backup and the newness of the phone, it is not surprising that the FBI's cursory review of the cellular phone did not yield any images of Victim 1 and Victim 2.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

50. Based on my training, experience, and information obtained from other agents, I know the below statements are accurate.

51. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

52. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as WiFi or Bluetooth. Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

53. Any computer can connect to any smartphone, tablet, or other computer. Through the internet, electronic contact can be made to millions of computers around

the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

54. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - computer hard drives, external hard drives, CDs, DVDs, and thumb, jump, or flash drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

55. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

56. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with

access to the internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

57. Individuals commonly use smartphone and computer apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

58. Communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

59. Based on my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain

characteristics common to individuals interested in a sexual relationship with children. Characteristics common to people interested in having a sexual relationship with children include that they:

a. Generally have a sexual interest in children and receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect sexually explicit or suggestive materials in a variety of media, including in hard copy and/or digital formats. People with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sex, or to demonstrate the desired sexual acts.

c. May also keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's underwear or other items belonging to a child.

d. May take photographs that either constitute child pornography or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and video may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

e. Generally, maintain their communication indicating a sexual interest in children and child pornography in a safe, secure, and private environment, most often where they live and/or on their person. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the individual's family.

f. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from others with a sexual interest in children; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same sexual interest in children. Such correspondence may take place, for example, through online bulletin boards and forums, internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person.

BACKGROUND CONCERNING EMAIL

60. In my training and experience, I have learned that Yahoo! Inc. provides a variety of on-line services, including electronic mail ("email") access. Yahoo! Inc. allows subscribers to obtain email accounts at the domain name yahoo.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Yahoo! Inc. During the registration process, Yahoo! Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo! Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo! Inc. subscribers) and information concerning subscribers and their use of Yahoo! Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

61. A Yahoo! Inc. subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Yahoo! Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

62. In my training and experience, Yahoo! Inc. generally ask their subscribers to provide certain personal identifying information when registering for

an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

63. In my training and experience, Yahoo! Inc. typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Yahoo! Inc. often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

64. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Yahoo! Inc. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

65. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the Yahoo! Inc. can show how and when the account was accessed or used. For example, as described below, Yahoo!

Inc. typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

66. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo!, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized

persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

67. Probable cause exists to believe that federal criminal laws, including matters involving violations of 18 U.S.C. §§ 2252 and 2252A, which make it illegal to distribute, transport, receive, possess, and access, with intent to view, child pornography have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A.

68. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the warrant. The government will execute the warrant by serving it on Yahoo! Inc. Because the warrant will be served on Yahoo! Inc., who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

69. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).